Legislative Proposals and Technological Threats in the Netherlands

Bart Scheffers
Tilburg School of Economics & Management, Tilburg University, Tilburg, Netherlands
b.c.scheffers@tilburguniversity.edu

Steven Hendriks
Tilburg School of Economics & Management, Tilburg University, Tilburg, Netherlands
s.hendriks_1@tilburguniversity.edu

Dhylan Simons
Tilburg School of Economics & Management, Tilburg University, Tilburg, Netherlands
d.t.a.simons@tilburguniversity.edu

Simeon ter Velde
Tilburg School of Economics & Management, Tilburg University, Tilburg, Netherlands
s.a.tervelde@tilburguniversity.edu

ABSTRACT

This paper focused on identifying which characteristics of a Technological trend impede the creation of legislative proposals in the Netherlands, which often is behind on technological trends and takes a significant amount of time in the Dutch legal system. We take a closer look at how these proposals are created and which requirements they should adhere to. Additionally, we explore the concept of a threat is and how to identify its characteristics and apply this to the case of DeepFake. These characteristics are then linked to proposals requirements where they might cause a bottleneck, after which these hypotheses were validated through an interview with an expert. Results show that privacy and adaptability are no issue, whereas the government's knowledge, ease-of-use of the technology and international boundaries are problematic characteristics in creating legislation. At the end limitations of the paper are discussed and future research directions suggested.

Keywords

Dutch Legislation, Legislation Proposal, Technological Threat, Threat Assessment

INTRODUCTION

Over the years technological trends have become a significant force in modern society, with effects reaching as far as the geopolitical sphere (Winner, 1995). One such trend is DeepFake, manipulated audiovisual videos in which people, often celebrities, world leaders or well-known individuals, are impersonated using Machine Learning algorithms. This forms a source of fun and entertainment, but also one of harassment or misrepresentation. A recent example from the political world is one where Barack Obama was impersonated, and seemingly criticized Donald Trump (Vincent, 2018). The technology can also be used to create Fake news, to misinform society about certain events or subjects (Albright, 2017), which is likely to have significant societal influence as well as impact societal trust (Fisher, 2018).

These examples show that the capacity to create DeepFakes is not likely to stay in the hands of technologically sophisticated or responsible actors. Any individual with a smartphone already has access (Porter J. , 2019). Since the technology is developing at a high pace, it can be questioned what this means for citizens' protection from such technological trends in the future. Legislation surrounding these new technologies, however, is currently unavailable or outdated, implying that current laws fall short in counteracting or adapting to technological developments to protect or support its citizens (Harris, 2019). Dutch law, for example, does not allow electrical hoverboards and monowheels to be ridden in public while it does allow ownership (Rijksoverheid (A), 2019), which does not allow people to make use a sustainable mode of transport. Even though the technology has been around for a while, Dutch law has not been able to adapt to this change in environment.

The question then is, why is Dutch law currently unable to adapt to technological changes, specifically threats? Looking at the complexity of this case, a background on both the Dutch Legislative process and the definition of a technological threat are needed.

Dutch Legislative Process

The legislative process applied by the Dutch government consists of several steps, which are partly defined in article 81 to 88 of the Dutch constitution (Voermans, 2016). It starts with an initiative from a policymaker which may be triggered by jurisprudence or societal pressure. The initiative is followed by the design of a legislative proposal with feedback from "Raad van State" (RvS), an advising body within the government.

This proposal is finally presented to the parliament for approval. This procedure may be repeated several times until the law is approved (Rijksoverheid (B), 2019). After approval, the law is implemented and enforced. The entire process takes on average two and a half up to three years, of which the approval phase takes around one and a half year (Voermans, 2016). The proposal phase of the legislation thereby spans one year up to one and a half year. This indicates that drafting a new law takes up a significant amount of time. Relating this to high paced technological trends presents the issue of timeliness, as many laws will be outdated by the time they are implemented (Wadhwa, 2014).

Technological Threats

A technological trend that may be a threat is characterized by a high likelihood of threatening "actions". The "action" is executed by an agent, which may or may not be a person, and is targeted towards other entities, usually involving individuals or their possessions (Steinberg, 2005). Additionally, there needs to be a malicious intent. A threat is assessed by the likelihood or frequency that such a situation occurs. If the likelihood is high, then the trend can be considered a threat. According to Steinberg (2005) identifying a technological threat requires one to look at the background and the potential threat of a technology and investigate its characteristics.

PROBLEM STATEMENT AND RESEARCH QUESTIONS

Knowing that 1) Dutch law is outdated from the hoverboard example, 2) the legislative proposals take a significant amount of time, and 3) what makes a technological threat, it seems plausible that some aspects of a technological threat impede legislative proposals. Based on this notion the research question of this study is defined as follows:

"Which characteristics of a technological threat negatively influence the legislative proposal procedures in Dutch law?"

To answer this research question, the following sub-research questions were developed:

Theoretical Research Questions:

- What are the procedures for a legislative proposal in Dutch law?

- What are the characteristics of a technological threat?

- Which characteristics of a technological threat are most likely to negatively influence Dutch legislative proposal procedures?

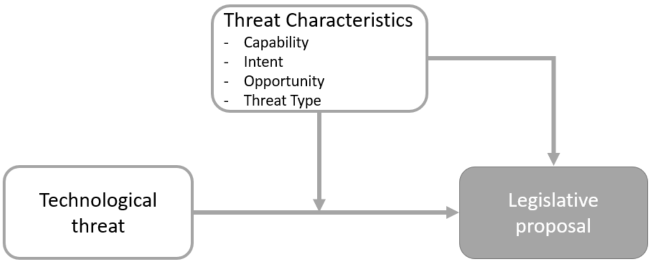
Practical Research Questions:

- To what extend does the relationship between technological threats and legislative proposals depend on threat characteristics?

THEORETICAL BACKGROUND

The main variable of interest is the legislative proposal. We specify two drivers of this dependent variable, namely Technological Threat and Threat Characteristics. The overarching label "Threat Characteristics" comprises capability, intent, opportunity and threat type. These constructs were developed by Steinberg (2005) and will be elaborated on individually. The conceptual model of this research can be found in Figure 1.

Figure 1: Conceptual Model



Legislative Proposals

Within the legislation proposal drafting process, which is part of the legislative process, many different procedures and associated quality requirements must be considered. Therefore, the integrated assessment framework for policy and regulation (IAK) serves as both a methodology and a source of information to aide in the drafting of legislative proposals (Ministerie van Justitie en Veiligheid (B), 2019). The IAK consist of seven questions with augmented documentation and corresponding quality requirements which can be found in Table 1. Only quality requirements that would apply to legislation surrounding technology are considered in this study.

As can be seen in Table 1, before a legislative proposal is approved and adopted, many different quality requirements should be met. Legislators must therefore consider many different criteria and domains before a law is considered for implementation. To get a better view on what each requirement entails, all quality requirements that apply to legislation about a technological trend are outlined in Table 2. The proposal will be tested against these quality requirements further in the process before approval (Rijksoverheid (C), 2019).

Table 1: IAK Policy and Regulation Framework (Ministerie van Justitie en Veiligheid (B), 2019) (Ministerie van Justitie en Veiligheid (C), 2019)

IAK Questions	Explanatory Notes	Quality Requirements
What is the cause?	The urgency, the context, and the political importance of the dossier; The first perspective from which a policy proposal is formulated; The factors that play a role in answering the other IAK questions.	Regulatory guidelines
Who are the stakeholders?	Identifying all parties of interest in terms of issues, interests, potential, and interrelationships.	Regulatory guidelines Business impact assessment (including regulatory burden effects) Assessment framework for inter-governmental relations Manual for regulating regulatory costs Feasibility and enforceability (U&H)
What is the problem?	In defining current or potential problems consider the different perspectives from stakeholders.	Regulatory guidelines
What is the purpose?	Formulated objectives should be clear to be interpreted and be categorized in three levels: Strategic, Specific, Operational	Regulatory guidelines Business impact assessment (including regulatory burden effects)
What justifies government intervention?	Government intervention must be justified by the existence of a public interest. The following questions should be answered: - Is there a task for the national government? - Is redistribution of wealth necessary? - Is there a reason to correct behavior? - Is there a market failure?	Regulatory guidelines Business impact assessment (including regulatory burden effects) Manual for regulating regulatory costs
What is the best instrument?	Policy instruments should be based on the following integral considerations: Legality, Effectiveness, Efficiency, Feasibility.	Regulatory guidelines Manual for regulating regulatory costs Framework Overview of Infrastructure Effects Privacy impact assessment
What are the repercussions?	Social cost-benefit analysis (SCBA) Repercussions should be categorized for: Civilians, Companies, and Government	Regulatory guidelines Business impact assessment (including regulatory burden effects) Assessment framework for intergovernmental relations Manual for regulating regulatory costs Measurement: passing on the costs of admission and enforcement Feasibility and enforceability (U&H)

Table 2: Legislation Quality Requirements (Ministerie van Justitie en Veiligheid (A), 2019)

Quality Requirements	Explanatory Notes
Regulatory guidelines	Requirements for the design of legislation and regulations and the process in which they are created
Business impact assessment (including regulatory burden effects)	How the effects of proposed legislation on companies can be made clear, prevented or kept as limited as possible
Assessment framework for intergovernmental relations	Standards and test points for the quality of intergovernmental relations with a role for provinces and municipalities
Manual for regulating regulatory costs	How to measure, describe, prevent or limit regulatory costs of proposed legislation for businesses and citizens
Report of the interdepartmental legislative deliberation on experimental provisions	Framework of conditions with which experimental provisions in legislation must comply
Principles for the choice of the sanctioning system	In legislation, the choice of a sanctioning system (criminal law, administrative law or a dual system) has to be justified on the basis of a number of factors. For instance, the actual chance of getting caught, or nature of the offence
Conformity assessment and accreditation in the context of government policy	Framework for the use of conformity assessment as a policy tool
Measurement: passing on the costs of admission and enforcement	Framework for passing on authorization and enforcement costs to individuals
MKB-assignment	Assesses the workability and feasibility of the legislative or regulatory proposal and its impact on the regulatory burden of SME companies.
Privacy impact assessment	Tool to assess to what extend new technology, information systems, programs, policies and legislative proposals meet privacy requirements.
Feasibility and enforceability (U&H)	Tool to identify intended and unintended consequences of draft regulations for the organizations affected by their implementation.

Technological Threat

No consensus on the concept “threat” exists, as its contextual, depending on the individual’s or organization’s characteristics and current situation. Additionally, little research has been done to accurately define the term. For this research we use the following definition: “A threat is defined as any act, entity, event or phenomenon with the potential to harm a person or thing.” (Deng, 2015). A technological threat there is any technology which has the potential to harm a person or thing. This includes both physical and psychological harm.

Threat Characteristics

Alan N. Steinberg (2005) has developed a Threat Assessment Model which helps identify potential threats in technological trends. The threat analysis was developed to establish a systematic approach for predicting, detecting and characterizing threat activity. Threats are modeled in terms of potential and actualized relationships between threatening entities and threatened entities, also targets. The model can be used for several different functions, but we will focus on identifying signs and characteristics in a technological trend and analyzing how it could become a threat. This assessment process evaluates the trend’s capability, intent and opportunity to be a threat.

The three elements should be described per technological trend to assess the likelihood of the trend being a threat. This will provide a basis for recognizing useful relationships between entities, targets, agents, and the threat. Additionally, threat type is also identified for a better understanding of what kind of threat is dealt with.

1. Capability: this element will look at the underlying technology of a trend and assess whether this technology has the inherent capability to design, develop, deploy or deliver the technology in a harmful way.

2. Intent: this element focuses on the intention of the trend. Different levels of threat objectives are considered, such as national, regional, local or individual. This helps in assessing the impact and prioritization of threats. (National Research Counsil, 2013)

3. Opportunity: this aspect identifies the frequency and likelihood of "opportunities" the technology has to be an effective threat against targets. The target's accessibility and vulnerability are also considered.

4. Type of threat: characterizes in which domain the technological threat falls, such as Political, Economic, Social, Technological, Environmental and Legal, based on the PESTEL model (Richardson, 2006). This is an important aspect in the assessment model for understanding the threat.

DeepFake Case

Now we will apply the threat assessment model of Steinberg (2005) to the technological trend DeepFake, to create a better characterization of the trend. The elements of capability, opportunity, threat type and intent will be outlined separately.

Capabilities

The first capability is Generative Adversarial Networks (GAN), which is based on neural networks. A neural network can be defined as a class of model within the general machine learning literature. This network is able to create accurate models when it processes a broad array of examples, and that way can create audio, video, or images that seem realistic (Anderson & McNeill, 1992). GAN brings two neural networks to bear simultaneously. The GAN-approach uses one network, known as the generator, which draws on a dataset to produce a sample that mimics the dataset. It uses the other network, called the discriminator, to assess the degree to which the generator succeeded. With this method each algorithm can train itself against the other, allowing GANs to produce highly realistic yet fake audio-visual content (Chesney & Citron, 2018).

The second capability is high adaptability. A GAN-approach has as effect that when a fake is discovered, the algorithm can correct itself to produce better ones. This makes it harder to discover in the future. Every discovery of a fake makes the technology better, making it highly adaptable.

The third capability is the technology's low dependency on inputs unlike most technologies. It only needs to access knowledge about approaches to machine learning, like Generative Adversarial Networks, and a few initial examples of what is right and wrong (Chesney & Citron, 2018).

Combining the GAN network, high adaptability and scarce dependency on inputs is what creates a high capability for DeepFake to be threat. The underlying technology can easily be used for harmful actions, and it only becomes better when fakes are discovered.

Opportunity

The first opportunity is ease of use. DeepFake has become popular due to the quality of tampered videos and the easy-to-use applications for a wide range of users with various computer skills, from professional to novice. This ease of use combined with the diffusion of the technology strongly increases the target's accessibility and vulnerability. Commercial and even free services have already appeared in the open market. The spread of these services will eventually lower the barriers to entry (Porter M. E., 2008). Furthermore, the overall increase in Social Media use makes this even more harmful (Veer, Boekee, & Hoekstra, 2019).

The second opportunity is target vulnerability. Individuals and businesses can face forms of exploitation, personal sabotage and intimidation due to DeepFake. These harmful activities are amplified by the fact that businesses and Dutch citizens cannot rely on Dutch law for protection. Moreover, Dutch society may also be a target. The damage can extend to distortion of democratic discourse on important policy questions; manipulation of elections; erosion of trust in public and private institutions; enhancement and exploitation of social divisions; harm to military or intelligence operations or capabilities; and damage to international relations. In short, target vulnerability is high. (Chesney & Citron, 2018)

Intent

The technology has high-level objectives, since it is a threat on national level. It can endanger public safety and/or disrupt international relations. Another reason why it has high-level objectives is because this technology can be classified as a cyber threat. The desirable targets of this threat and its effect on them can mainly be classified as destructive (Chesney & Citron, 2019).

Threat Type

The type of threat depends on the characteristics of the threat, it can be classified as one of the six dimensions of the PESTEL model

(Richardson, 2006). Deep Fake can be categorized as a technological threat since it is based on AI technology. To be more specific, it can be classified as a cyber threat. A cyber threat is a threat that is controlled by a person who is unauthorized to access a system and use data for another purpose than intended. A cyber threat is often associated with the use of data and personal information, which constitute potential security and privacy risks (Probst, Hunker, Gollmann, & Bishop, 2010). Evidence for cybercrime is often hard to uncover since collection of data proof difficult. Besides that, it will rarely withstand in court (Grimes, 2016).

Linking DeepFake to Legislative Proposals

Observing DeepFake characteristics while taking the legislative process into account, there are several aspects that stand out and are presumed to lead to issues when proposing new legislation. First, dealing with risks and incidents is becoming increasingly complex for policymakers. On one hand, society wants less government regulation, while on the other hand it expects more guarantees of safety (Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, 2015).This makes defining the reason for government intervention, the fifth IAK question, a complex and lengthy process. It is arguable whether government intervention is necessary for DeepFake, as no significant damage has occurred because of it until now.

Second, because DeepFake can keep learning and adapt itself, with the help of GAN's, it is questionable whether the requirement "feasibility and enforceability" can be met. This can be a logical explanation why there has not been a regulation, which counteracts DeepFake, in the past. As said before the GAN-characteristic can develop itself without human intervention. This results in the problem that it is unclear who is responsible from an enforcement perspective. In addition, the fact that the technology spreads and operates across international borders adds more complication, since there are limitations in international lawsuits.

Third, another reason why enforcement may be difficult, may be due to the ease-of-use of the technology. DeepFake is readily available for anyone with a smartphone in the form of apps, making it nationally accessible. Enforcement of regulations regarding such widespread technology is difficult, as the current enforcement tools of the government does not allow control to such an extent (Ministerie van Justitie en Veiligheid (A), 2019).

Forth is legality. Nowadays, a large amount of data, such as pictures and videos, are accessible online and can be used as input for DeepFake, which then produces new content often without consent. From a legislative perspective this may be privacy infringement (privacy quality requirement). However, it can also be argued that it does not affect privacy, since the use of publicly available data, like pictures and videos, is not prohibited, creating issues around privacy in drafting new legislation.

Fifth and last is cyber threat. Enforcement is one of the problems when proposing new legislation around cyber threats. This is due to the difficulty of gathering legal evidence. Bulletproof evidence of cyber-crime is hard to get. Obtaining the right evidence requires a lot of skills and resources. Judges, as well as officers, must be educated too. Additionally, most cyber-crimes are not reported and therefore accurate statistics are hard to come by, even though they are necessary for successful prosecution.

METHOD

To gather a solid base for the theoretical background, pre-research was conducted through a literature review, was formed our secondary data. The research's data is qualitative and aims to provide in-depth information. This is needed due to the exploratory nature of the research. We aim to explain the causes and consequences of a problem.

The findings in the theoretical background are then used to formulate presumptions. These are then validated by conducting semi-structured interviews with a cybersecurity and law experts. This is the primary data of our research. Semi-structured interviews were chosen as it allows for flexibility and deeper questioning during the interviews. Additionally, this method aides in gathering in-depth information which is needed to better understand the nature of technical threats as well as the law-making process, and the links between the two. The presumptions made based on the theory serve as a basis of the interview guide.

Judgmental sampling was used to select interviewees, as specific knowledge within the field of Law and/or Cybersecurity is needed. The initial sample size chosen for this study was 5, to get the minimum information required to answer the research question. After the fifth interview the saturation method was applied, meaning that we continued interviewing relevant experts until study results reached data saturation.

In order to assure validity and reliability in the interviews, several techniques were used. First, the theoretical background was well-researched, and questions were developed based on this information. Secondly, during the interview the interviewers used a funneling technique in which they asked open-ended questions in the beginning, which become progressively more focused as the interview continued. Other measures to ensure validity specifically included: asking unbiased questions, clarifying questions, taking notes.

The results derived from the interviews are analyzed going through the following steps; 1) Transcribing and preparing the interview; 2) coding and describing data point; 3) conceptualization, classifying, categorizing, identifying themes; 4) connecting and interrelating data 5); interpretation and providing meaning (Hoyos & Barnes, 2012).

RESULTS

DeepFake has currently not caused any problems for Dutch citizens, therefore there isn't any legislation yet. Many governmental institutions including policy makers will generally only pay attention to it after it caused damage. Looking at the current level of expertise at governmental institutions, knowledge regarding technological threats, its characteristics and the right repercussions is missing.

The rapidly changing characteristics of a technological threat are not considered to be a problem since law enforcement makes regulations based on the output of a process. In this way the same legislation can be applicable to many different cases and will last longer. Since a computer or machine can't be hold responsible, the provider of the output will be held responsible for its content. However, problems can occur when this provider is located out of The Netherlands. Although new legislation has the legitimate right to hold the provider responsible, without the cooperation of other countries' law enforcement, it will be hard to enforce Dutch legislation. Even when cooperation exists, collecting the appropriate amount of evidence will be hard.

DeepFake is widely available for other purposes than crime, which makes the hard line of crime more difficult to determine. This strict line, however, needs to be elaborated in detail when creating a legislative proposal in order to make enforcement of the legislation possible.

Privacy is considered not to be a problem when proposing new legislation. The law enforcement is allowed to use a proportionate amount of private data in order to protect citizens against crime. This has already been registered in the GDPA legislation.

DISCUSSION

The rapidly changing characteristics of a technological threat do not make it harder to propose new legislation with regards to technological threats. Laws are designed to be applicable to many cases and therefore focuses on the output of the threat. The provider of the output of the threat will be held responsible and therefore the fact that this threat have been created by machine learning algorithm makes no difference compared to threats directly created by humans.

Legislation regarding technological threats require international legislation, just like the GDPR, because of the international character of cybercrime. Legislation only in the Netherlands will not be adequate to enforce a criminal from outside The Netherlands, and thus may harm Dutch citizens. This is a potential issue when creating new legislation.

Determining the hard line of crime appeared to be much harder when the ease of use of a technology is high. Determining the hard line of crime requires expertise of law enforcement to determine the specific characteristics which are considered a crime. Without the right expertise it's impossible to fulfil the requirements to successfully propose new legislation. The new legislation will be not be enforceable when these characteristics are not correctly defined beforehand. The fact that this expertise is lacking also shows from the fact that proposals are mainly introduced after a threat has caused damage for the first time. It can be concluded that the right expertise to forecast threats is missing.

Privacy can be thought of as a sensitive topic and therefore a problem when proposing new legislation. The GDPA, however, already gives authorities the rights to use personal data for law enforcement purposes against potential threats.

However new legislation to protect citizens against technological threats, is lacking. It will be unknown what the future will bring us but when investigating the DeepFake case it can be concluded that there are already laws protecting Dutch citizens from the output, the fake content, which is the actual danger of DeepFake. For instance, using public data to create a Deep Fake is enforceable, since it is considered a copyright violation.

CONCLUSION

This research has several contributions. First, by identifying which characteristics form and obstacle in legislative proposals and which do not we may facilitate the improvement of the legislative. Knowing which issues to address or avoid can help in speeding up the legislative process. For the DeepFake case specifically, this research has shown that Dutch citizens are already well protected by law through privacy and copyright laws. Secondly, this research can be used as an example for future research, involving more diverse technological trends with characteristics dissimilar to DeepFake.

Potential limitations of this research are shown in the fact that only the Dutch legislative proposal process is considered. This research will therefore only be relevant for the Dutch government and is not directly applicable for other countries, as each country's legal system and laws differs significantly. Additionally, in this research we only focus on potential negative influence on the proposal process, whereas positive influences may have provided additional insights and relevant characteristics. Another limitation is the sample size used to conduct the research, as only one expert was interviewed.

Although the research is not directly applicable to other countries, characteristics of a technological threat are generalizable and can be suggested as a basis of future research for governments or researchers in other countries. Moreover, the process after the proposal, the ‘’approval’ process, may also be researched, in order to aide faster implementation. Another suggestion is to dive deeper into the bottlenecks shown in this research and determine how to prevent them. Lastly, further research should provide more insights in the adequacy of current laws regarding technological threats, and whether it might be possible to adjust this legislation instead of proposing new legislation.

REFERENCES

Albright, J. (2017). Welcome to the Era of Fake News. *Media and Communication*, 87-89.

Anderson, D., & McNeill, G. (1992). *Artificial Neural Networks Technology.* New York: Kaman Sciences Corporation.

Chesney, R., & Citron, D. (2019). Deepfakes and the New Disinformation War. *Foreign Affairs*, 147-156.

Chesney, R., & Citron, D. K. (2018). Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security. *107 California Law Review (2019, Forthcoming); U of Texas Law, Public Law Research Paper No. 692; U of Maryland Legal Studies Research Paper*.

Deng, Y. (2015). A Threat Assessment Model under Uncertain Environment. *Mathematical Problems in Engineering*, 12.

Fisher, C. (2018). What is meant by 'trust' in news media? *Trust in Media and Journalism*, 19-38.

Grimes, R. A. (2016, December 6). *Why it's so hard to prosecute cyber criminals | CSO Online.* Retrieved from CSO | Security news, features and analysis about prevention, protection and business innovation.: https://www.csoonline.com/article/3147398/why-its-so-hard-to-prosecute-cyber-criminals.html

Harris, D. (2019). Deepfakes: false pornography is here and the law cannot protect you. *Duke Law & Technology Review*, 35.

Hoyos, M. d., & Barnes, S.-A. (2012, February 15). *Slide 1.* Retrieved from https://warwick.ac.uk/fac/cross_fac/esrcdtc/coretrainingmodules/quals/analysing_interview_data_1_-_w6.pdf

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties. (2015). *Handreiking Bestuurlijk Balanceeren met Risico's en verantwoordleijkheden.* Den Haag: Rijksoverheid.

Ministerie van Justitie en Veiligheid (A). (2019, 10 31). *Beleidsinstrumenten A-Z | Kenniscentrum Wetgeving en Juridische zaken*. Retrieved from Welkom op Kenniscentrum Wetgeving en Juridische zaken | Kenniscentrum Wetgeving en Juridische zaken: https://www.kcwj.nl/kennisbank/integraal-afwegingskader-beleid-en-regelgeving/6-wat-het-beste-instrument/61/index?cookie=yes.15731266765111466031415

Ministerie van Justitie en Veiligheid (B). (2019, 4 23). *Integraal afwegingskader voor beleid en regelgeving | Kenniscentrum Wetgeving en Juridische zaken*. Retrieved from Welkom op Kenniscentrum Wetgeving en Juridische zaken | Kenniscentrum Wetgeving en Juridische zaken: https://www.kcwj.nl/kennisbank/integraal-afwegingskader-voor-beleid-en-regelgeving

Ministerie van Justitie en Veiligheid (C). (2019, November 3). *Aanwijzingen voor de regelgeving | Kenniscentrum Wetgeving en Juridische zaken*. Retrieved from Welkom op Kenniscentrum Wetgeving en Juridische zaken | Kenniscentrum Wetgeving en Juridische zaken: https://www.kcwj.nl/kennisbank/integraal-afwegingskader-voor-beleid-en-regelgeving

National Research Counsil. (2013). Climate and Social Stress. In N. R. Counsil, *Climate and Social Stress* (pp. 139-160). Washington DC: The National Academies Press.

Porter, J. (2019, September 2). *Another convincing deepfake app goes viral prompting immediate privacy backlash - The Verge*. Retrieved from The Verge: https://www.theverge.com/2019/9/2/20844338/zao-deepfake-app-movie-tv-show-face-replace-privacy-policy-concerns

Porter, M. E. (2008). The Five Competitive Forces that Shape Strategy. *Hardvard Business Review*, 23-41.

Probst, C. W., Hunker, J., Gollmann, D., & Bishop,

M. (2010). *Insider threats in Cyber Security.* Springer.

Richardson, J. J. (2006). The library and information economy in Turkmenistan. *IFLA Journal*, 131-139.

Rijksoverheid (A). (2019, October 31). *Mag ik met een hoverboard, elektrisch skateboard of monowheel op de openbare weg rijden? | Rijksoverheid.nl*. Retrieved from Informatie van de Rijksoverheid | Rijksoverheid.nl: https://www.rijksoverheid.nl/onderwerpen/bijzondere-voertuigen/vraag-en-antwoord/hoverboard-op-openbare-weg

Rijksoverheid (B). (2019, November 5). *Hoe komt een wet tot stand? | Wetgeving | Rijksoverheid.nl*. Retrieved from Informatie van de Rijksoverheid | Rijksoverheid.nl: https://www.rijksoverheid.nl/onderwerpen/wetgeving/hoe-komt-een-wet-tot-stand

Rijksoverheid (C). (2019, November 5). *Kwaliteit van wetten en regels | Wetgeving | Rijksoverheid.nl*. Retrieved from Informatie van de Rijksoverheid | Rijksoverheid.nl: https://www.rijksoverheid.nl/onderwerpen/wetgeving/kwaliteit-wetten-en-regels

Steinberg, A. N. (2005). Threat Assessment Technology Development. *Modeling and Using Context*, 490-500.

Veer, N. v., Boekee, S., & Hoekstra, H. (2019). *Nationale Social Media Onderzoek 2019.* Newcom Research & Consultancy B.V.

Vincent, J. (2018, April 17). *Watch Jordan Peele use AI to make Barack Obama deliver a PSA about fake news - The Verge*. Retrieved from The Verge: https://www.theverge.com/tldr/2018/4/17/17247334/ai-fake-news-video-barack-obama-jordan-peele-buzzfeed

Voermans, W. (2016). Commentaar op artikel 82 van de Grondwet. *Artikelsgewijs commentaar op de Grondwet*. Netherlands.

Wadhwa, V. (2014, April 15). *Laws and Ethics Can't Keep Pace with Technology - MIT Technology Review*. Retrieved from MIT Technology Review: https://www.technologyreview.com/s/526401/laws-and-ethics-cant-keep-pace-with-technology/

Winner, L. (1995). *Democracy in a Technological Society.* Dordrecht: Kluwer Academic Publishers.